

Tatort Internet

Woche 2: Digitale Identitäten



Dilemma schwacher Passwörter

Prof. Dr. Christoph Meinel

Hasso-Plattner-Institut
Universität Potsdam

Schwache Passwörter

Viele Nutzer verwenden bei Einrichtung ihrer digitalen Identität bei einem Dienst im Internet **schwache Passwörter**

Grund: „Menschlicher Faktor“ (Human Factor)

- Bequemlichkeit
- Komplexe Passwörter sind schwer zu merken
- Fehlendes Sicherheitsbewusstsein
- ...

Passwörter können aus verschiedenen Gründen **schwach** sein:

- 1. Zu geringe Komplexität**
- 2. Ableitbar aus Nutzerkontext**
- 3. Wiederverwendung** bereits genutzter Passwörter

Schwache Passwörter: Passwörter mit geringer Komplexität



Wann sind Passwörter schwach?

- Weniger als 12 Zeichen
- Verwendung nur einer Zeichengruppe (Zahlen, Buchstaben, Sonderzeichen)
- Tastenfolge auf Tastatur, z.B. „qwertz“, „qwe123“, ...
- Auffindbar in einem Wörterbuch
- Kriterien für „starke“ Passwörter können abweichen

→ siehe auch **Exkurs: Passwortlänge** in dieser Woche

#	Passwort	Häufigkeit
1	123456	8.01 ‰
2	123456789	3.84 ‰
3	password	1.87 ‰
4	qwerty	1.82 ‰
5	12345	1.36 ‰
6	12345678	1.15 ‰
7	111111	1.14 ‰
8	qwerty123	1.00 ‰
9	1q2w3e	0.95 ‰
10	123123	0.84 ‰

Quelle: HPI Identity Leak Checker

- Tabelle zeigt **Top 10 der meistgenutzten Passwörter** basierend auf Klartext-Leaks im HPI ILC

Schwache Passwörter: Passwörter aus dem Nutzerkontext

- Viele Nutzer verwenden persönliche Daten als Passwörter
 - Name, Vorname,
 - Name des Partners / Kindes / Elternteils
 - Geburtsdatum
 - Lieblingsband oder Fussballverein
 - ...

 - Teilweise werden Passwörter auch nach jeweilig genutztem Dienst gewählt
 - Adobe Datenbank: adobe123, photoshop, adobe1, ...
- **Angreifer, der sein Opfer kennt, kann solche Passwörter leicht erraten**

Schwache Passwörter: Wiederverwendung von Passwörtern

Viele Nutzer verwenden relativ sichere Passwörter, **aber:**

- Gleiches Passwort wird oft für verschiedene / alle Accounts verwendet, z.B.
 - ***D7\$4?g!inRo*** wird bei der Anmeldung für jeden Dienst verwendet
- **Wird Passwortdatei nur eines Dienstes geleakt, dann sind auch alle anderen Dienste betroffen**
- Wird Passwort nur leicht abgewandelt für unterschiedliche Accounts verwendet, kann das zu schnellerem Erraten führen
 - ***D7\$4?g!inRo*A** für Dienst **A**
 - ***D7\$4?g!inRo*B** für Dienst **B**
 - ...

Wahl Sicherer Passwörter

- Keine Informationen aus dem **Nutzerkontext** verwenden, also keine Informationen, die Angreifer über ihr Opfer recherchieren können, z.B.
 - Name, Vorname, Geburtsdatum, Lieblingsband, ...
- Keine Wörter aus einem **Wörterbuch** oder **Sprichwörter**
- Mindestens **12 Zeichen** lang
- Passwortzeichen aus **verschiedenen Zeichengruppen** wählen (Sonderzeichen, Groß- und Kleinbuchstaben, Ziffern)
- Verwendung **unterschiedlicher Passwörter** für unterschiedliche Accounts
- Keine Wiederverwendung alter Passwörter
- Passwortmanager nutzen (siehe W2-8 Passwordmanager)
- **Schutzmaßnahme: Gute Passwörter** in dieser Woche